Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.3, No.10, 2013
www.iiste.org

A Novel Technique for Secure Information Transmission in Videos Using Salt Cryptography

Nagesh Sharma, Dr. Rakesh Rathi , Vinesh Jain, Mohd. Waseem Saifi
Government Engineering College, Ajmer , Rajasthan , India

Abstract

This paper presents a new technique for transmitting secret information securely from one party to another by embedding this information into a video after encryption through salt cryptography. We have tried to utilize the advantages of salt cryptography which has been ignored by data hiding community. In this encryption method some random data is added to the secret keys and passwords. We will define this random data as a salt which is needed to access the encrypted data, along with the password. Alone these passwords have no use since they will be able to locate the hidden data only when mixed with proper salt. This salt is managed by a certified third party. Different salt is created for different pairs of communicating parties. The purpose of salt is to add arbitrary random data to the string being hashed, such that you increase the length of input to hash. We have also introduced the concept of Enterprise Dependent Value (EDD), which are the embedding values corresponding to the binary digits and are specific to the communicating enterprises. The effectiveness of the techniques has been shown through experimental results. The performance of the proposed technique has been compared with the other techniques of watermarking, steganography and encryption.

Keywords: Cryptography, Decryption , Encryption , Salt, Steganography , Video watermarking.

1. Introduction

In the past decade one of the greatest technological advancement is to change people lives has been the internet. Digital multimedia data and content over the web are spreading through various channels. Nowadays it has been noticed that by making illegal copies of data some people are misusing and leaking the information which creates a bad environment in the field of software industry. The problem of protecting multimedia information becomes more and more important, as we have witnessed in the past few months. The need to maintain the availability of multimedia information secures new algorithm need to be developed.

To protect the data so that it can be distributed over the internet without being error prone lead to the concept of information hiding. Information hiding is used in a wide variety of applications, information hiding can be done in text, audio, video and multimedia data. There are various techniques for information hiding such as cryptography, steganography, digital watermarking [1]. In this paper our focus will be on Steganography.

Steganography is the art and science of hiding the secret information in such a way that only the recipient is aware of existence of message. The word steganography comes from Greek word ‘stegano’ which means covered and graphia means writing. In steganography a message is hidden in a carrier that may be a text, image, audio, and video. It is transmitted over a communication channel in such a way i.e. the existence of message is hidden .The goal of steganography is to hide message inside the carriers in a way that attacker cannot detect the presence of message [2]. Steganography is an excellent way of information hiding it can be combined with cryptography to add various levels of security to a system. There are certain key differences between steganography and cryptography. Steganography means “cover writing” while cryptography means “secret writing” [3]. In cryptography a message is transmitted to the intended receives in such a way that only the receiver is able to decode the original message .The plain text is converted to cipher text and transmitted over a communication channel. Only the intended receiver can convert the cipher text back to original message. While in steganography the message is embedded inside the data which acts as a carrier. The lack of strength in cryptographic system motivated the development of new technique called steganography.

2. Related Work

For secure communication many techniques have been proposed in the last few years that provide an efficient way of transmitting the required secret information by using video steganography. The steganography has found its applications in a wide variety of areas, it has a significant contribution in military and government organization

The paper [4] proposes an algorithm which is a combination of two highly secured techniques MD5 for cryptography and DCT for steganography. An information security scheme is proposed using Cryptic

steganography. Cryptography and steganography are combined for secret communication using three keys named as cryptic steganography system which avoid the problem of unauthorized data access.

In paper [5] author proposed a steganographic method which is based on biometrics, that uses a skin region of images in DWT domain for embedding secret data. They introduced an image cropping concept which maintain a security at respectable level, so cropped region works as a key at decoding side. Since no one can extract message without having value of cropped region.

The author [6] designs a stego machine to develop steganographic application using LSB (Least Significant Bit) method. They proposed a method which is useful for hiding the data in to video images and to retrieve the hidden information from the video using LSB (Least Significant Bit) modification method. A modified least significant bit coding method is used which provides a low computational complexity and high watermark channel bit rate. In this method each pixel has room for 3 bits of secret information, one in each RGB values. By using this method it is possible to hide up to 2,359,296 bits.

An algorithm [7] is proposed as an efficient approach towards steganography which describes image as a shared key between sender and receiver which stores the secured text. The characters in the text are converted into binary and then mapped for every pixel value in the image. The image can be recovered using index array which contains the indices for hidden data. It is not possible to reconstruct the image from index array, if eavesdropper has stolen the information because the shared image is still unknown to the eavesdropper. Divide and mean method is used to increase the complexity of index array.

The paper [8] presents a secure data hiding algorithm using encrypted secret message. By using simple encryption algorithm and secret key the hidden message is encrypted. The secret message is encrypted before embedding process starts. A simple encryption algorithm is used to hide the encrypted message which makes it impossible for the attacker to unhide the secret message. In this paper author proposed an N-bit and LSB (Least Significant Bit) substitution technique which is used as embedding and extraction method.

3. Overview of the proposed algorithm

In this section we will explain the proposal for secret message hiding in the video file for secure transmission of the secret message. The complete package of the algorithms can be divided into three major tiers, Sender Tier (First party), Receiver Tier (Second Party), Authenticating authority (Third Party).
Each of the communicating parties has specific task to do and for this they have limited information. It is to be noted that no party has all the information content and the secret information stored at a place. So a successful communication can only happen in one case only if the all the parties are together communicating.

3.1 Information at the Communicating Parties

Table1: Information content of the communicating parties

Sender Tier		**Receiver Tier**		**Third Party (TP)**
Sender	**Sending Module**	**Receiver**	**Receiving Module**	
Own User id	Salt from TP	Own User Id	Salt from TP	Salt for sender receiver pair
Own Password	Receiver password from TP	Own password	Sender password from TP	Both login id and corresponding passwords but in encrypted form
Receiver user id	EDD from TP	Sender id	EDD from TP	EDD for the pair
Video to communicate		Video to communicate		

The table below shows which information is contained with which party. The Sender and receiving tiers have two sub tiers. First sub-tier consists of the sender and receiver themselves. On the second tier the software module which is connected to the third party (TP) is placed. Once the person is authenticated by TP then software module automatically imports all the information required for the particular pair from TP.

3.2 Enterprise Dependent Values

These are the intensity values that are specific to the pair of communicating parties. These values will be embedded into the video frames at the locations decided by the combinations of the secret password and the random salt.

3.3 Text to binary conversion

We have incorporated a simple character to binary conversion using the ASCII equivalents of the characters. The characters in the message string are stored in the ASCII format in the computer. So we have taken the ASCII corresponding to the message characters and converted that number into the binary equivalents 8 bit strings. All the 8 bit equivalents of the characters are concatenated together to make the final binary message. The length of this binary message will now be considered as the binary message length for number of frames requirements.

3.4 Number of Frames required

The minimum number of frames required is greater than or equal to the number of characters in the message We have adopted strategy for 1 character per frame since even if one frame is deleted by the attacker only one character will be lost and the word can still be completed using the dictionary software taking relevant word from the available combinations.

3.5 Salt Cryptography

The purpose of salt is to produce a large set of keys corresponding to a given password among which one is selected as a random. To make decryption less efficient for attacker's salt is used in cryptography by adding another hashing layer on the top of an encryption algorithm. . Salt can also be added to make it more difficult for an attacker to break into a system if an attacker does not know the password and is trying to guess it with a brute force attack, than every password he tries has to be tried with each salt value. If the salt has one bit this makes the encryption twice as hard to break in this way, and if the salt has two bit this makes it four times as hard. A three bit salt makes eight times as hard, if the salt is 32 bits long for instance there will be many as 2 ^ 32 keys for each password you can imagine how difficult to crack passwords with encryption that uses a 32 bit salt. The only security requirement of salt is that they are unique per user.

3.6 Salt Size

The Salt used for Steganography is exclusive for the pair of the sender and the receiver. Different pairs will have different salt. The salt is generated using a seeded PN sequence generator by the third party to which both sender and receivers should be registered. We have included the idea of salt since it increases the complexity of the localization of the message inside the video frames.

4. Proposed Algorithm

4.1Algorithm Steps

Once all the information has been collected the encoding and decoding process starts. Now we will discuss the detailed steps of the proposed algorithm.

4.1.1 Third Party Authentication

- **i.** Both the sender and the receiver registers themselves to third party
- **ii.** They register with a unique user id and a password
- **iii.** Third party selects a Enterprise Dependent value (EDD) and unique salt sequence which is unique for the pair of sender and receiver
- **iv.** This EDD value and salt is unknown to both sender and receiver.
- **v.** User id and passwords are not stored in original format at the servers of third party; instead they are kept in secure encrypted format.
- **vi.** Overall, it can be visualized as any of the first, second or third party not knows all the information required for the location of the message inside the videos.
- **vii.** Every time the users will communicate after getting authenticated by third party.

4.1.2 Sender side

- **i.** The system should be installed with the sender module.
- **ii.** Input the secret message to be sent to the receiver into the secret message.dat file.
- **iii.** Sender login with its own id and password to the third party**.**
- **iv.** Sender enters the desired receiver id to which he wants to send the data.
- **v.** Sender selects an irrelevant video to its message field to hide the message into it.
- **vi.** The text message to be sent hidden in the video is converted in to ASCII binary value string.
- **vii.** Installed module gets the EDD value corresponding to the user id and receiver id combination. These are two values EDD1 and EDD0 for '0' and '1' bits respectively.
- **viii.** The video is divided into frames.
- **ix.** The number of frames in the video should be equal to at least the message character length including spaces.

a. If the message length is greater than frame length error will prompted**.**

x. Binary salt length and width is decided by the sender module
- **a.** Length= number of bit length of message
- **b.** Width = log(video_ height* video_ width)-1

xi. Receiver id and password is converted into binary string of length= number of bit length of the message.

xii. Merge salt and binary receiver id and password.

xiii. For every bit in message find position in the video frame using decimal value of (salt + binary receiver id & password) and place either EDD0 or EDD1 depending on message bit value '0' or '1'.

xiv. After every eight message bits take new frame, so that 1 frame has only 1 character.

xv. Calculate CRC of video and send CRC with the video**.**
- **a.** The CRC generator polynomial is created using first 4 characters of the receiver's password.
- **b.** A CRC sequence of all the frames of the Stego video is created so that any forging during the communication of the message can be counterfeited.

4.1.3 Receiver Side

i. The system should be installed with the receiver module.

ii. Input sender id from which the communication is expected.

iii. Input receiver id and password**.**

iv. Calculate CRC of received video and compare it with the CRC send by the sender.

v. Receiver id and password are converted to binary ASCII string**.**

vi. Get the salt from the third party corresponding to the pair of the sender and the receiver.

vii. Merge salt and binary receiver id and password.

viii. Location of embedded EDD values is known using decimal values of the combined salt and binary receiver id and password.
- **a.** if [location]= EDD1 then message bit=1
- **b.** else if [location]= EDD0 then message bit =0
- **c.** else video is not correct, so discard video

ix. Combine 8 message bits to form an ASCII character**.**

x. Move to next frame for next character.

xi. Join all the characters to make the complete message

The following architecture of the proposed algorithm gives the brief details of the process. The three tiers of the method are shown properly**.**

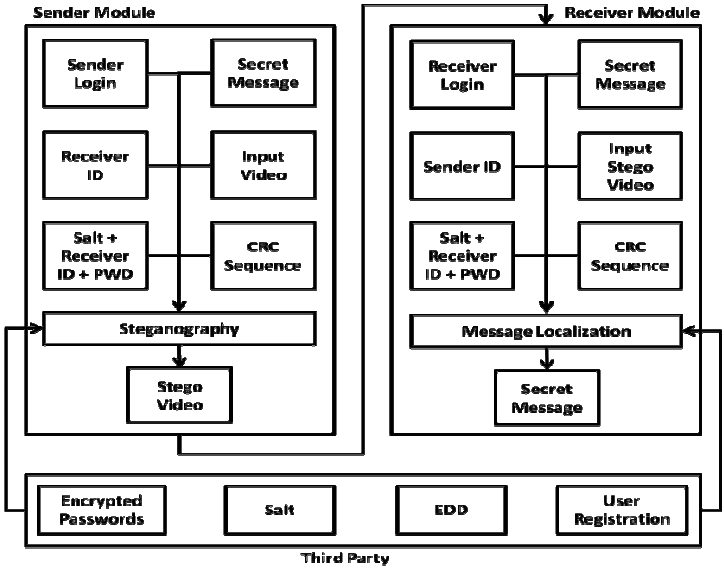

Figure 1: Schematic view of algorithm

4.2 Attacks on the Stego Video

There are various attacks that can be applied on any cryptographic system especially when some data is hidden into the medium. Here we will discuss these attacks in context of secret data hiding in the video only. Major attacks on video steganographic systems are listed below. We are also discussing how our proposed method is preventing these attacks.

4.2.1 Frame Deletion Attack

In frame deletion attack, the attacker deletes frame for the original message. The lost message can be recovered at the receiver because each frame contains one alphabet of the message which can be formed by using 26 combinations of the English alphabets and by forming a logical term from the dictionary.

4.2.2 Forgery Attack

In forgery attack the original message is captured by the eavesdropper which in turn transmits another message in place of the original one. This way the communication parties are not able to communicate properly. In our method some eaves dropper cannot forge the data since this will change the CRC of the video frames and ultimately CRC fail will occur leading to rejection of the video.

4.2.3 Replay attack

In replay attacks communication stream between two parties is captured by an adversary, and replayed to produce unauthorized effect. In our proposed method if the video is stored by the eavesdropper C and then it replays it then it will not be played since the parties A and B will be using session salts. It is generated randomly every time a video is created and known to third party only. All the salts are different from each other for different transmissions. Third party keeps it active only for some pre-decided time; later this salt expires and will not be given to the receiver. So if the video is tried to be decrypted after the specified time it is assumed to be replayed and it will not be considered valid.

4.2.4 Eavesdropping

An eavesdropper or adversary is a malicious entity whose goal is to prevent the communicating parties from achieving their objectives. We prevent eavesdropping by simply the password authentication combined with the salt cryptography. The password alone is not capable of localizing the data in the video. It requires the salt to be combined with the password to get the exact location but this salt has been received from third party for registered users only. So the eavesdropper cannot know the exact locations of the message.

4.2.5 Brute Force attack

In this attack the attacked tries for all possible permutations of the frame pixels to get the message, but we don't embed the actual message bits into the video file. We only embed the EDD values in the video which are in intensity domain like the other pixels. So mathematically it is impossible to predict the EDD values and to retrieve the message without knowing the exact embedding locations.

4.2.6 Malicious communicating parties

If any of the communication parties are malicious then they can share the secret information. But in our proposed methodology all the information is not known to a single party. All the parties know only their domain of information. So even if they leak their part of information then the secret data is secured since the secret data from other parties also required for retrieval of the secret message from the video.

5. Simulation Results

Experiments are carried on a computer system, having Intel P4 processor 3.06 GHz clock and 4 GB RAM. After breaking the video into frames, a color component has been chosen into which the message is embedded. The simulation tool is MATLAV v7.8. We have used the functions for video processing on the uncompressed AVI format. Secret information will be kept in windows DAT file and supporting information will be stored in the MATLAB data files.

5.1 Secret message input

The secret message that the sender wants to send to the receiver is kept in a data file. We are not taking it from the console since it should not be visible to everyone. The person responsible for the secret message can give this message file input to the sender module. This text will be read from the file and will be converted into binary message string. This string will now be the secret information to transferred and embedded into the video frames.

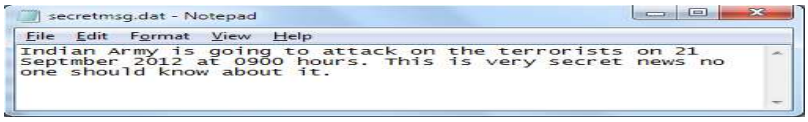

Figure2: Secret message data file

5.2 Peak Signal to noise ratio

Since very small number of pixels has been disturbed it does not lead to any visible difference in the video. This disturbance can be quantified using the PSNR metric which measures the embedded noise in one signal with respect to the original signal. Here embedded signal is our stego video and original signal is the video in which the embedding has been done.

We calculate the average PSNR of all the embedded frames with their respective original frames. This average values for different videos have been checked and infinite value suggests that there is no visual noise in these two frames.

The PSNR is calculated as follows:

$$PSNR = 10 log_{10}\left(\frac{255^2}{MSE}\right) dB$$

$$\text{where } MSE = \frac{1}{A_p \times B_p} \sum_{I=0}^{A_p-1} \sum_{J=0}^{B_p-1} (X(i,j) - X_W(i,j))^2$$

where X and X_W are the original and watermarked images respectively of size A_p x B_p represent the height and width of the images. X'_W represents the extracted watermark.

5.3 Histogram Comparison of the frames before and after the data

Following histograms represents the frequencies of the various intensities in a randomly chosen frame before and after the embedding. There is no difference in the histograms. The peaks are same in both so a histogram comparison cannot predict that the data is contained in the video and our secret message is safe.

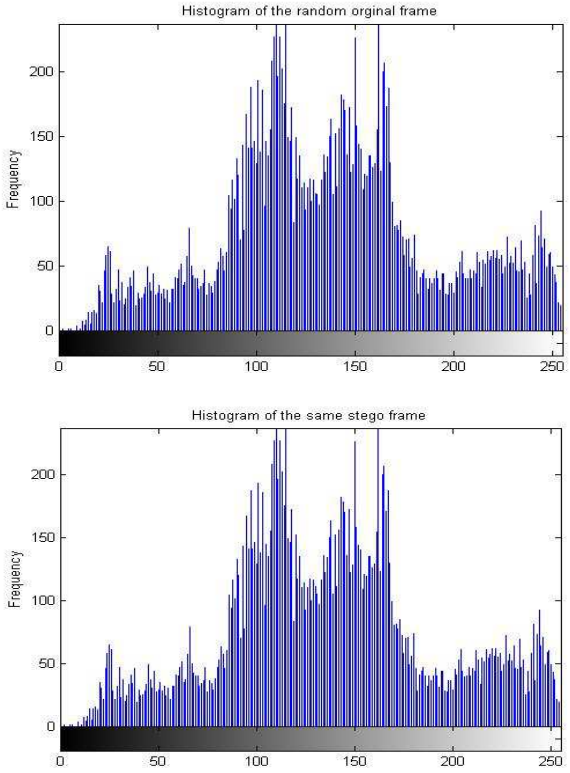

Figure 3: Histogram comparison of the original and Stego frame

5.4 Visual comparison of frames

The randomly selected frame from the original video and same frame from the Stego video are shown in the figure below. There is no visually perceptible difference in the images. This shows the effectiveness of the proposed algorithm.

Figure 4: Original and Stego frame

5.5Message Output

The message is not stored anywhere for the security point of view. It is just displayed for the sake of security. Once the message is seen is will be flushed from the buffer and to see gain the whole decoding process has to be repeated.

```
Video is authentic

hiddenmsg =

Indian Army is going to attack on the terrorists on 21 Septmber 2012 at 0900 hours. This is very improtant news all should know about it.
```

Figure 5: Output Message**.**

6. Performance against Attacks

6.1 Frame Deletion

```
Video is authentic

hiddenmsg =

Indi n Ar y is goin  to  ttac  on  he t rror sts  n 21 Sept ber  012  t 09 0 ho rs.  his  s ve y im rota t ne s al  sho ld k ow a out  t.
```

Figure 6: Output Message extracted after frame deletion

Frame deletion with a rate of 1 frame per 5 frames has been chosen. Still all the words can be recognized by simply using the dictionary. From 150 frames 30 frames have been deleted still the message is quite understandable. This we have obtained after ignoring the CRC fail.

6.2 Eavesdropper

When an eavesdropper tries to attack on the video, he will not be able to see the message. But if he wants to change the contents of the message he can do by embedding useless information or some noise into it. Since the video has been disturbed the CRC sequence of the video will not match and a CRC error will occur. This indicates that the video should be discarded.

```
Error using receiver (line 88)
CRC Check Failed cannot proceed futher
```

Figure 7: CRC failure when the video is tampered

7. Comparison with other Schemes

7.1 Scheme 1

The technique proposed by [9] for transmitting the required secret information by embedding secret message into the video after encryption. This algorithm uses a 512 bit key value for encryption and localizing of secret information in the video. This technique is similar to us but the difference is that it encrypts the secret message which makes this approach complex. In our approach we use Salt cryptography which is also an encryption

method but it is only to increase the complexity of the attacker to detect the message even if he knows the secret passwords. Our approach is very less complex due to lack of message encrypting yet more secure.

7.2 Scheme 2

The proposed method in [10] creates an index for the secret information and the index is placed in a frame of the video itself. This is obviously an overhead for the video which gives low PSNR values in comparison to our work. With the help of this index, the frames containing the secret information are located. So if this information is lost due to some attack then the secret information cannot be located inside the frames. Also in both the approaches the no one is claiming the message security when the video is tampered in that case there will be false detection in these methods but our method will simply reject the video instead of giving wrong information. During the extraction process, instead of analyzing the entire video, the frames containing the secret data are analyzed with the help of index at the receiving end. This is also risky so here we have used the sequential frames to reduce stored information overhead.

7.3 Analysis

Many of the approaches explained used for data hiding have many superior results to share with the data hiding research world. But most of them are concentrating on the image processing attacks. We are mainly concentrating on the video processing attacks that we mentioned in detail in the previous chapter. Another important thing to note is that we are storing minimal information inside the video so the quality of the stego video is very high even it has pages of data stored in it. One character per frame helps us to attain robustness against the frame deletion attack. Other attacks are also ineffective against our method as shown in the simulation results and are justified with appropriate reasoning. The most common replay attack yet most harmful can easily be abandoned through our approach since the authentication of the random salt is from the TP. Salt cryptography is very much effective since it is least complex but adds so much data into the secret keys so that it is impossible to detect the correct embedding location.

Table 2: Attack Summary

Sr. No.	Attack	Detected characters	Explanation
1.	No Attack	150	All the characters are detected properly
2.	Frame Deletion (30 frames deleted)	120	One character per frame deleted yet the message is readable
3.	Replay Attack	None	Video Rejected since the salt expired
4.	Eavesdropping	None	Salt + sender_ info + receiver_ info not known together to eavesdropper
5.	Forgery Attack	None	CRC fails so video rejected
6.	Malicious Communicating Nodes	None	Any node does not have all the information to localize secret message
7.	Brute force	None	EDD value not known to compare with pixel intensities

8. Conclusion and Future work

This scheme is novel in this area and has no algorithmic comparisons. The concept of salt cryptography and EDD are completely novel. We are also using framed video data hiding method so we have compared our results reported by some papers in this area. The results are very good as there is no visual change in the Stego video and the PSNR values are also coming infinite. The main idea to check the hidden data i.e. histogram checking is also not able to detect the presence of the data. Extra involvement of CRC prevents any tampering of this video. So overall this approach is successful landmark for data hiding in the videos. We are planning in future to include some frequency domain transforms to make it comparable with other techniques in the frequency domain.

References

Fabien A.P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. “Information hiding- A Survey”, Proceeding of IEEE, special issue on protection of Multimedia content ,July 1999,pp.1062-107.

L.Y. POR, B.Delina: Information hiding: A New Approach in Text Steganography , 7th WSEAS Int. Conf. On Applied Computer and Applied Computational Science(ACACOS 08) Hangzhou, China, April 6-8 , 2008

Sabu M Thampi: Information hiding Techniques: A tutorial Review, ISTE-STTP on Network Security & Cryptography, LBSCE 2004

B. Raja Rao, P. Anil Kumar, K Rama MohanaRao, M. Nagu, : A Novel Information Security Scheme using Cryptic Steganography in Indian Journal of Computer Science and Engineering Vol. 1 No. 4 327-332.

Anjali A.Shejul, Prof. U.L Kulkarni: A DWT based approach for Steganography using Biometrics, in IEEE 2010 International Conference on Data Storage and Data Engineering.

Mritha Ramalingam , Stego Machine- Video Steganography using Modified LSB Algorithm in the World Academy of Science , Engineering and Technology 74 2011.

Rupinder Kaur, Mandeep Kaur , Rahul Malhotra, A New Efficient Approach towards Steganography in International Journal of Computer Science and Information Technologies, Vol. 2 (2), 2011, 673-676.

Harshita K M, Dr. P. A. Vijaya ,Secure Data Hiding using Encrypted Secret message in International Journal of Scientific and Research Publication, Volume 2, Issue 6, June 2012 .

LoveleshSaxena, AnujTewari K.V. Arya, “A Novel Technique for Secure Information Transmission using Framed Video Watermarking”, Image Processing and communication challenges3 Advances in Intelligent and soft computing Volume 102,2011,pp245-256

R.Balaji ,G. Naveen , “Secure data Transmission using Video Steganography”in 2011 IEEE International conference on Electro/Information Technology(EIT).